DOCID 4125072

TOP SECRET
SECURITY INFORMATION

DETERMINATION OF THE ABSOLUTE SETTING OF THE AM 1 (M-209)* BY USING TWO MESSAGES WITH DIFFERENT INDICATORS

1. It is presupposed that the following technique is known: the determining of the absolute setting by means of a decrypted message, whose relative setting has been found.

2. For the second message a new apparatus of strips has to be made. The preparation of the strips (with the effective pin and alphabet sequences) is made analogously to the base of the first message--each set of strips being made independently of the other.

3. In determining the absolute setting by using one indicator group every possible setting of each rotor is tested against the assumed pin sequence until a setting free from contradictions on all rotors is found. This is also true in the case of using two indicator groups except that here the letters of each two corresponding rotors are arranged--in respect to each other in each coupled setting of the apparatus--so that the same letter on each rotor is in the same position in the effective pin sequence. The arrangement of these letters on the rotors is shown in Table III.

4. The advantage of using two indicator groups lies in the simultaneous use, from the beginning of the analysis, of both sets of strips, whereby, with respect to any one indicator group, a greater number of assumed settings can be recognized as impossible.

---

* DF-105
TICOM Doc. 2795

SECURITY INFORMATION

Declassified by NSA 06-12-2014 pursuant to E.O. 13526 FOIA Case# 77972

DOCID: 4125072

~~TOP SECRET~~
SECURITY INFORMATION

5. First, the initial rotor setting of the second message with respect to that of the first message must be sought--the position of which will be arbitarily noted as A A A A A A (the relative effective alignment of message 1).

6. The first message (designated herein by CAPITAL letters)* has, for example, the indicator group TTEGF CEBTL. The strips for each rotor may be seen in Table I.

7. The second message (designated herein by lower case letters)* has, for example, the indicator group vvnp daktl. The strips for each roto may be seen in Table II.

8. Now lay the strip for the 26-rotor of the second message beside the strip of the 26-rotor of the first message so that the same portions of the effective pin sequences are in alignment. Then, boginning at the first of the strip of the 26-rotor of the first message, count the interval of the alphabet sequence (in normal order) of that rotor to the place where the start for the 26-rotor of the second message appears. In this example the letter "V" will be found. (See Table II A).

9. The strips for all the other rotors are treated in the same manner, and the following letters are found:

rotor	26	25	23	21	19	17
letter	V	L	V	N	L	P

---

* In the original the first message was designated by "BLUE" letters and the second message by "RED" letters.

SECURITY INFORMATION

10. These letters determine the rotor settings of the second message in respect to the rotor settings of the first message. That is, "A" on rotor 26 of the first message corresponds to "V" on rotor 26 of the second message. "A" on rotor 25 of the first message corresponds to "L"L on rotor 25 of the second message, etc. The order of the other letters of the different rotors can be seen in Table III.

11. The determination of the absolute setting by means of both sets of strips is performed as follows: In the set of strips for the first message the 26-rotor will be set to "E" and in the strips for the second message the 26-rotor will be set to "z". (See Table III). In each set of strips the sign arrangement of the pin sequence for the corresponding letters is taken from the appropriate "kick" table (See Table VI, VII), and entered in the spaces over "E" and "z" respectively. In Message I the 25-rotor strip sign is "plus"; in Message II it is likewise "plus". Now in Message I the 25-rotor-strip is entered at "E". The corresponding letter on the 25-rotor-strip of Message II should be "p" (See Table III). However, in Message II this setting is not possible since a "minus" sign is alloted to the letter "p", while on account of the sign arrangement entered over "z" only a "plus" sign is possible.

12. The next possible setting of the 25-rotor-strip must be investigated. This setting is "D", "o". Since now in both sets of strips several impossible "w's" are to be found (Table IV, V) the 23-rotor strip is used in order to facilitate the

elimination of impossible letters. The first possible setting of the 23-rotor-strips is "E", "c". Since, in the set of strips of the first message, the sign arrangement of the pin sequence "plus minus, plus"*, which appears in the second vertical column, is not to be found among the impossible "w" letters of the 25-rotor, only the letter "D" can appear in this position. In the "kick" table (Table VI) this sign arrangement of the pin sequence is found under the letter "D". Likewise in the strips of the second message no "w" is possible and the sign order "minus, plus, plus", appearing in the second column, is to be found in Table VII at "ω". Now, in both sets of strips, it must be tested whether or not the setting of "E", "c" will be possible with impossible letters in the 23-rotor. Since in both sets of strips it still seems possible for such letters to appear, the number of these possibilities may be narrowed by means of the strip for the 21-rotor.

13. On the 21-rotor strip "C" of the first message is set against "p" of the second message, which produces a contradiction in the strips of the second message. The next assumed setting for the 21-rotor-strip is "O", "g", whereby in the strips of the second message a contradiction still appears, since in the strips of the second message the sign arrangement "plus, minus, plus", (in the third column) is out of the question

---

* The Germans listing of these rotors is always in a descending order. In the above example the rotors are the 23rd, 25th, and 26th. This will be true throughout the translation. The ASA usage is to list the 26 rotor first.

TOP SECRET
SECURITY INFORMATION

either for an impossible letter on the 23-rotor (Table V) or for "c" (Table VII).

14. The next setting to be investigated on the 21-rotor is "J", "b". This, too, is impossible since in the strips of the first message by inspection of the third and fourth columns (see Table IV, VI) this case can be excluded. Further possible settings of the 21-rotor-strip of the first message are not valid. Therefore, the next possible "minus, plus" arrangement for the first message is set up on the 23-rotor-strips. This is "P" "n". Since there are, at first, four impossible patterns to be found in the strips of Message I, and 3* impossible patterns in the strips of Message II, the 21-rotor-strip is used again. In the setting "O", "g" of the 21-rotor-strip, the sign arrangement of "plus, plus, plus plus", appearing for Message II in the third column, can be found neither for an impossible letter of the 23-rotor (Table V) nor under the letter "n" (Table VII). This setting is therefore impossible.

15. The next setting on the 21-rotor is "J", "b". Here, too, it develops in the strips for the second message, that the 23-rotor, as well as for the 21-rotor, no impossible letters appear, but in the third column "n" appears and in the fourth column "b" appears. On the other hand, in the strips for the first message, in the third column an impossible letter appears,

---

* The original has "2" here (zwei verbotene Buchstaben) but this is an error because there are three. The text has therefore been corrected.

105

DOCID: 4125072

~~TOP SECRET~~
SECURITY INFORMATION

and in the fourth column "p" is possible. For the impossible letter in the third column there are two possibilities: "W & Z". Therefore one turns directly to the 19-rotor-strip.

16. By using both sets of strips there develops as the next possible setting on the 19-rotor "L", "d". In the strips for Message II one finds in the fifth column that "d" is determined by the sign arrangement "plus, plus, plus, plus, minus". Since, in the strips for Message I, in spite of the addition of the 19-rotor, several impossible letters still appear, the strip for the 17-rotor is set up immediately, so that, by using both sets of strips, the setting "Q", "o" is obtained, whereby, now, all the rotors are determined without any question.

17. After that, one finds the indicator groups:

E D Z P J Y L Q

z 0 n b d ɛ o

18. The rest of the procedure, viz., assigning the correct letter to each sign of the pin sequence, is the same as in the procedure for <u>one</u> indicator group.

DOCID: 4125072

TABLE I

17 b a q p o n m l k j i h g f e d c
- ≠ ≠ ≠ ≠ - - ≠ - - - ≠ - - ≠ ≠ ≠ - ≠ ≠ ≠ ≠ - - ≠ - - - ≠

19 e d c b a s r q p o n m l k j i h g f
- ≠ - - - - ≠ ≠ ≠ - ≠ - ≠ - ≠ - ≠ - - - ≠ - ≠ - - - - ≠ ≠ ≠ - ≠ -

21 g f e d c b a u t s r q p o n m l k j i h
≠ - - - ≠ ≠ ≠ - - - - ≠ ≠ ≠ ≠ - ≠ - ≠ ≠ - ≠ - - - ≠ ≠ ≠ - - - - ≠

23 f e d c b a x v u t s r q p o n m l k j i h g
≠ - ≠ - ≠ - - - - ≠ ≠ ≠ - - ≠ ≠ - - ≠ ≠ - - - ≠ - ≠ - ≠ - - - - ≠ ≠ ≠

25 g f e d c b a z y x v u t s r q p o n m l k j i h
- - ≠ ≠ - ≠ - - ≠ - ≠ ≠ ≠ ≠ - - - - ≠ ≠ - - - - - - ≠ ≠ - ≠ - - ≠ - ≠ ≠

26 e d c b a z y x w v u t s r q p o n m l k j i h g f
- ≠ - ≠ ≠ - - ≠ - - ≠ ≠ ≠ - - - - - - ≠ ≠ ≠ ≠ ≠ ≠ - ≠ - ≠ ≠ - - ≠ - - ≠ ≠

TABLE II

17 k j i h g f e d c b a q p o n m l
≠ ≠ - ≠ ≠ ≠ ≠ - - ≠ - - - ≠ - - ≠ ≠ ≠ - ≠ ≠ ≠ ≠ - - ≠ - ≠

19 a s r q p o n m l k j i h g f e d c b
- ≠ - ≠ - - - ≠ - ≠ - - - - ≠ ≠ ≠ - ≠ - ≠ - ≠ - - - ≠ - ≠ - - - -

21 d c b a u t s r q p o n m l k j i h g f e
≠ ≠ - ≠ - ≠ ≠ - ≠ - - - ≠ ≠ ≠ - - - - ≠ ≠ ≠ ≠ - ≠ ≠ - ≠ - - -

23 p o n m l k j i h g f e d c b a x v u t s r q
- - ≠ - ≠ - ≠ - - - - ≠ ≠ ≠ - - ≠ ≠ - - ≠ ≠ - - ≠ - ≠ - ≠ - - - - ≠

25 n m l k j i h g f e d c b a z y x v u t s r q p o
≠ ≠ ≠ ≠ - - - - ≠ ≠ - ≠ - - - - - - ≠ ≠ - ≠ - - ≠ - ≠ ≠ ≠ ≠ - - - - ≠ ≠ - -

26 p o n m l k j i h g f e d c b a z y x w v u t s r q
≠ ≠ ≠ ≠ ≠ - ≠ - ≠ ≠ - - ≠ - - ≠ ≠ ≠ ≠ ≠ - - - - - ≠ ≠ ≠ ≠ ≠ ≠ - ≠ - ≠ ≠ - -

TABLE II A

26 rotor
Msg 1:
a b c d e f g h i j k l m n o p q r s t u v
- ≠ - ≠ ≠ - - ≠ - - ≠ ≠ ≠ ≠ - - - - - - - ≠ ≠ ≠ ≠ ≠ - ≠ - ≠ ≠ - - ≠ - - ≠ ≠ ≠ ≠
≠ ≠ ≠ ≠ ≠ - ≠ - ≠ ≠ - - ≠ - - ≠ ≠ ≠ ≠

Msg 2:

DOCID: 4125072

TABLE III

Msg 1 for all rotors	26	25	23	21	19	17
a	v	l	v	n	l	p
b	w	m	x	o	m	q
c	x	n	a	p	n	a
d	y	o	b	q	o	b
e	z	p	c	r	p	c
f	a	q	d	s	q	d
g	b	r	e	t	r	e
h	c	s	f	u	s	f
i	d	t	g	a	a	g
j	e	u	h	b	b	h
k	f	v	i	c	c	i
l	g	x	j	d	d	j
m	h	y	k	e	e	k
n	i	z	l	f	f	l
o	j	a	m	g	g	m
p	k	b	n	h	h	n
q	l	c	o	i	i	o
r	m	d	p	j	j	
s	n	e	q	k	k	
t	o	f	r	l		
u	p	g	s	m		
v	q	h	t			
w	r					
x	s	i	u			
y	t	j				
z	u	k				

DOCID: 4125072

TOP SECRET
SECURITY INFORMATION

tt •gf gob tl Msg 1

TABLE IV

	W W W
17	≠ ≠ ≠
19	≠ – –
21	– – –
23	– ≠ –
25	– ≠ –
26	– – ≠

25
W
– ≠ ≠
≠

	W Z Y W Z W Z Y
17	≠ ≠ ≠ ≠ ≠ ≠ ≠ ≠
19	≠ – ≠ – ≠ – ≠ –
21	– ≠ – – – – – –
23	– – – ≠ ≠ – – ≠
25	– – ≠ ≠ ≠ – – ≠
26	– – – – – ≠ ≠ ≠

23
– ≠ ≠ W Y Z
≠ – –
≠ ≠ –

	W Z X V Y W Z W Z X X Y V
17	≠ ≠ ≠ ≠ ≠ ≠ ≠ ≠ ≠ ≠ ≠ ≠
19	≠ – ≠ – ≠ – ≠ – ≠ – – – ≠
21	– ≠ – – – – – – – – – ≠
23	– – ≠ – – ≠ ≠ – – ≠ – ≠ ≠
25	– – – ≠ ≠ ≠ ≠ – – – ≠ ≠ ≠
26	– – – – – – – ≠ ≠ ≠ ≠ ≠ ≠

21
≠ ≠ ≠ ≠ ≠ ≠ V W
– ≠ – ≠ – ≠ X Y Z
≠ – – ≠ ≠ –
≠ ≠ ≠ – – –

DOCID: 4125072

TOP SECRET
SECURITY INFORMATION

TABLE V

vv pnp dak tl
Msg 2

	W W
17	≠ ≠
19	≠ -
21	- -
23	- ≠
25	≠ ≠
26	- ≠

25
W

- -
- ≠

	Y	W	Z	Y	Y	W	Z
17	≠	≠	≠	≠	≠	≠	≠
19	-	≠	-	≠	≠	-	≠
21	≠	-	≠	-	-	-	-
23	≠	-	-	≠	-	≠	≠
25	-	≠	≠	-	≠	≠	≠
26	-	-	-	≠	≠	≠	≠

23
- ≠ - VW
- ≠ - X YZ
≠ - -

17	≠	≠	≠	≠	≠	≠	≠	≠	≠	≠	≠	≠
19	-	≠	-	≠	-	≠	≠	-	≠	-	≠	
21	≠	-	≠	-	≠	-	-	-	-	-	-	-
23	-	≠	≠	-	-	≠	-	≠	≠	-	-	≠ ≠
25	-	-	-	≠	≠	≠	-	-	-	≠	≠	≠ ≠
26	-	-	-	-	-	-	≠	≠	≠	≠	≠	≠ ≠

21

≠ ≠ ≠ ≠ ≠ -
≠ ≠ ≠ - ≠ - VW
≠ ≠ - - ≠ - XYZ
≠ ≠ ≠ ≠ - -

DOCID: 4125072

TABLE VI tt •gf geb tl
Msg 1

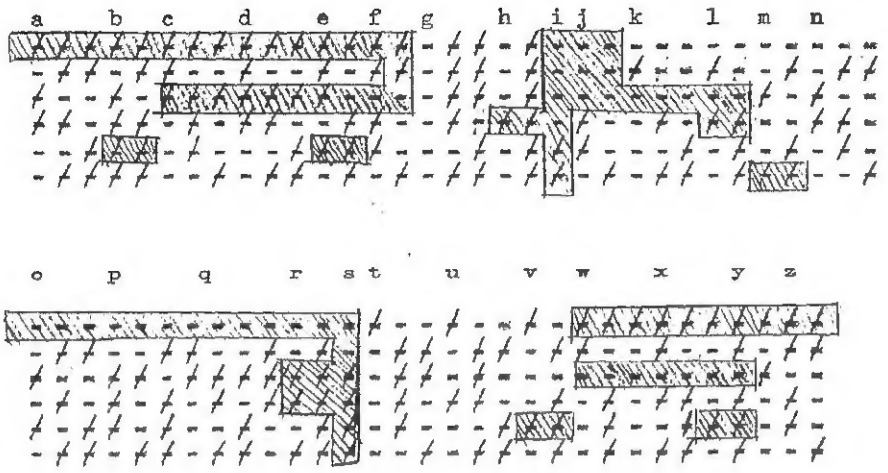
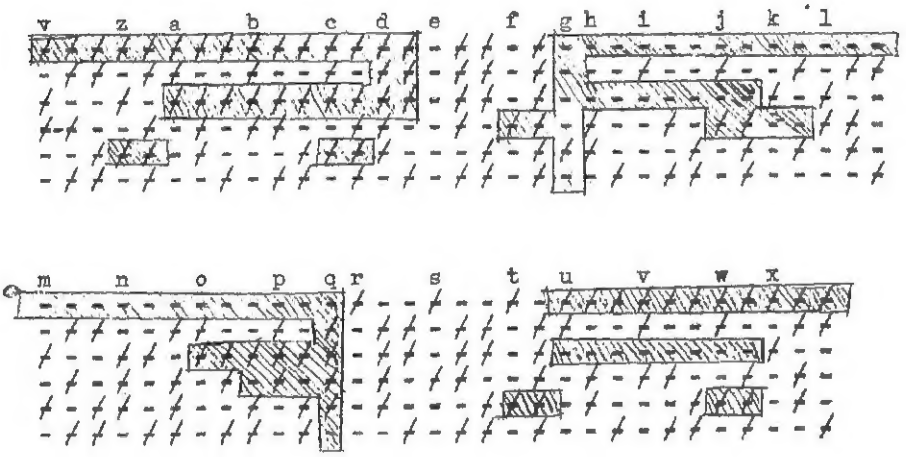
TABLE VII vv pnp dak tl
Msg 2